UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/911,750	07/23/2001	Charles M. Patton	10007237-1	4995

7590 08/23/2007

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
08/23/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/911,750	PATTON ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,14,15,21-27,31-34,36,37,42-44 and 47-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,14,15,21-27,31-34,36,37,42-44 and 47-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 13 June 2007 has been entered.

2. By the above submission, Claims 1-12, 14, 15, 21, 22, 25, 26, 36, 37, and 44 have been amended. Claims 13, 28-30, 35, 38-41, 45, and 46 have been canceled. New Claims 47-63 have been added. Claims 1-12, 14, 15, 21-27, 31-34, 36, 37, 42-44, 47-63 are currently pending in the present application.

Response to Arguments

3. Applicant's arguments filed 13 June 2007 have been fully considered but they are not persuasive.

Claims 1-15 were rejected under 35 U.S.C. 101 as directed to non-statutory subject matter. Claims 1-15, 21-35, and 37-46 were rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al, US Patent 6385596, in view of Fujiwara, US Patent

Application Publication 2001/0054081, and Stefik et al, US Patent 6233684. Claim 36 was rejected under 35 U.S.C. 103(a) as being unpatentable over Dwork et al, US Patent 6038316, in view of Fujiwara and Stefik.

Regarding the rejection under 35 U.S.C. 101, Applicant asserts that "the specific data processing function now recited in the claims defines a functional relationship that renders the claimed subject matter statutory" (page 13 of the present response). However, the Examiner notes that this is a mere allegation, as Applicant has not stated what that "specific data processing function" is. It appears that the claim language does not explicitly encompass any specific function; rather, the claim is still only directed to a digital file and a digital string embedded in that file. Although the claim includes the language "a data structure", it does not appear that the claimed "data structure" actually meets the definition of a data structure as set forth in MPEP § 2106.01, namely, as "a physical or logical relationship among data elements, designed to support specific data manipulation functions". As noted, Applicant has not stated what functionality is imparted by the alleged data structure. There is clearly not a physical relationship between the data elements; although the string is "embedded" within the file, this is not an actual physical embedding but a conceptual arrangement where the information of the string is included within the information of the file. There is also not a clear logical relationship between the data elements, and there is no specific data manipulation function that the file with the embedded string performs or supports. Although the claim recites that the string was embedded in the file, this embedding occurred previously, and is not a function that the file and/or string perform or would enable to be performed.

Further, although the claim recites that the file "is processable by a computer program... to reveal said embedded digital string", this merely recites a capability, and does not provide any specific functionality either. Therefore, the digital file and digital string, while they may have "independent value" and "latent value", respectively, as claimed, do not clearly provide for performing any particular data manipulation function; nor does the combination or arrangement of the file and string, particularly the embedding of the string within the file, appear to provide for performing any data manipulation function. Therefore, although Applicant cites a portion of MPEP § 2106.01 that states that functional descriptive material on a computer-readable medium constitutes a structural and functional interrelationship with the medium and is therefore statutory (see page 13 of the present response), the claim is still directed merely to an arrangement of data, which is non-functional descriptive material, and therefore is not statutory subject matter even though stored on a computer-readable medium.

As noted in the previous Office action, the Examiner again notes that, as per Office policy, a functional interrelationship would be defined if the claimed data, in conjunction with any claimed hardware, would realize a specific data processing function. An example of this would be computer code that included instructions for performing a particular method, where the code was stored on a disk or other computer readable medium, so that when the code was executed on a computer by reading the disk, the method would be performed. This would be a specific function to be performed, and the relationship between the code itself and the computer's hardware

and software components would be a structural and functional relationship. See MPEP § 2106.01 (and particularly MPEP § 2106.01 I).

Further, although Applicant has requested that the Examiner provide exemplary language for the claims that would be deemed to overcome the rejection, the Examiner submits that providing such language is not within the Examiner's purview or authority, nor is it the Examiner's duty or responsibility to rewrite Applicant's claims, especially as to substantive matters. The Examiner again notes that Claim 21 is directed to a method that includes substantially similar steps as performed in Applicant's example presented at page 12 of the response received on 20 December 2006. Because Claim 21 is directed to a method and therefore the steps are performed and produce a useful, concrete, and tangible result, Claim 21 is considered to be directed to statutory subject matter. However, the Examiner notes that instructions that perform the steps described above are not what is claimed in Claims 1 and 15. In contrast, Claims 1 and 15 are directed to the arrangement of the pieces of data that would result from such a method, rather than providing that functionality themselves. There does not appear to be any function recited that the arranged pieces of data (the file and embedded string) perform themselves.

Regarding the rejections under 35 U.S.C. 103(a), in response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Specifically, in reference to the

rejection of independent Claim 1, Applicant argues that none of the cited art, individually, suggests the provider making a key publicly available that is used to reveal the embedded string in clear form (pages 15-16 of the present response). However, the Examiner respectfully disagrees, noting that, although the relevant portions were not cited in the previous Office actions, the Examiner believes that at least Stefik discloses the use of public keys used for retrieving the watermark (i.e. embedded) information (see Stefik, column 16, line 51-column 18, line 5).

In response to applicant's argument that there is no suggestion to combine the references (page 17 of the present response, where Applicant alleges that the cited motivation is "too vague"), the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, although Applicant asserts that the previously cited motivation to combine the Wiser and Fujiwara references, namely to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049), is "too vague and not specific enough", this assertion is a mere allegation of patentability, because Applicant does not attempt to explain why this motivation is "too vague" nor the standard by which Applicant has attempted to judge the specificity of the motivation. Applicant merely makes the above statement without citing any specific evidence or reasoning in support of the assertion. The Examiner

maintains that because the specific motivation, as cited above, is found within the cited prior art, this provides a rational underpinning for a *prima facie* case of obviousness. In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning (also page 17 of the present response), it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

Further in reference to Claim 1, Applicant alleges that the Stefik reference teaches away from combination with the Wiser reference because Wiser outputs data in unprotected form and Stefik outputs data in protected form. Applicant further alleges that applying a watermark as taught in Stefik to the audio data of Wiser in order to create the protected data taught by Stefik would create an undesirable tradeoff between quality and protection (see pages 17-18 of the present response). First, the Examiner notes that the types of protection to which Applicant refers, namely the encryption in Wiser and the watermarking in Stefik, are not mutually exclusive. That is, while a document or file that was previously protected by encryption may be rendered in an unencrypted form (and thereby unprotected in that respect), this does not prevent the same file from being protected by a watermark. In fact, for the data to be comprehensible to a human user (who is reading a document or listening to an audio

file, for example), any encryption must, in fact, be removed, but this does not require that any watermarks must likewise be removed. Further, regarding the alleged tradeoff between protection and quality of an audio file, the Examiner asserts that it is well known that sophisticated watermarking techniques exist that enable a watermark to be inserted in virtually any type of data without noticeably degrading the quality), and that such a tradeoff mustn't necessarily be made. Additionally, although Applicant states that "'Trade-offs often concern what is feasible, not what is, on balance, desirable. Motivation to combine requires the latter'" (quoting *Winner Int'l Royalty Corp. v. Wang*, 53 USPQ2d 1580, 1587), the Examiner notes that the footnote following the above citation states that "The fact that the motivating benefit comes at the expense of another benefit, however, should not nullify its use as a basis to modify the disclosure of one reference with the teachings of another. Instead, the benefits, both lost and gained, should be weighed against one another". The Examiner asserts that even assuming, *arguendo*, that the tradeoff noted above would have to be made, the gain in security from the watermark may be desirable even in exchange for the loss of quality caused by the embedding of the watermark, dependent on the specific implementation.

In reference to independent Claim 37, Applicant refers back to the arguments in reference to Claim 1 (see page 18 of the present response). In response, the Examiner notes that the above responses referring to Claim 1 are applicable as appropriate to Claim 37.

In reference to independent Claim 15, Applicant argues that none of the references, individually, disclose the embedding of a provider digital string, and that

"another cited reference must disclose embedding the provider information in order to properly combine it with the Stefik reference" (see page 19 of the present response). However, Applicant provides no support or rationale behind this statement, and further, the Examiner believes that Stefik does, in fact, disclose embedding provider information in content data (see, for example, Stefik, column 3, lines 31-35, where a watermark, which is embedded data, includes information about the owner of the document, i.e. the provider). Regarding Applicant's further assertion that "information relating to the owner of a document is different from information relating to the provider of a document" (page 20 of the present response); Applicant alleges that the repository serves as the provider instead (citing Stefik, column 5, lines 64-66 and Figure 5, 501). However, the Examiner believes that because the owner provides the digital work to the repository, it is, in fact, the owner that servers as the provider of the document (see, for example, Stefik, column 5, lines 39-43, where it is the owner that attaches usage rights to the work).

In reference to independent Claims 21 and 44, Applicant argues that none of the cited prior art, individually, was cited to disclose the newly added limitation of embedding two different modified digital strings modified in two different manners (see pages 20-22 of the present response). However, the Examiner believes that the cited references do, in fact, disclose embedding different strings modified in multiple manners (see at least Stefik, column 8, lines 51-56, where multiple watermarking techniques may be applied).

In reference to independent Claim 36, Applicant argues that none of the cited art individually, and Dwork in particular, discloses the provider conveying an encryption key

to the public (pages 23-24 of the present response). However, the Examiner believes that the combination of Dwork, Fujiwara, and Stefik does, in fact, disclose the claimed limitation (see Stefik, column 16, line 51-column 18, line 5, where public keys are used for retrieving the watermark, i.e. embedded, information)

Further in reference to Claim 36, Applicant substantially repeats the arguments regarding insufficient motivation, the use of hindsight, and the allegation that Stefik teaches away from combination with Dwork for similar reasons as asserted regarding the combination of Wiser and Stefik in reference to Claim 1 (see page 25 of the present response). The Examiner directs Applicant's attention to the responses to those arguments in reference to Claim 1 set forth above.

Further, Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Specifically, 37 CFR 1.111(b) requires that Applicant's reply "must present arguments pointing out the specific distinctions believed to render the claims, **including any newly presented claims**, patentable over any applied references" (emphasis added). The Examiner notes that no arguments have been presented in reference to new Claims 47-63. However, because the present response appears to be a *bona fide* attempt at advancing the prosecution of the present application, the present response has been treated as though it were fully in compliance with the provision of 3 CFR 1.111.

Therefore, for the reasons detailed above, the Examiner maintains the rejections as set forth below.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 1-12, 14, 15, 62, and 63 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 1-12, 14, 15, 62, and 63 are directed merely to arrangements of data, although stored in a processor readable medium. Specifically, the independent claims recite a digital file and at least one digital string arranged as embedded within the file. An arrangement of data is non-functional descriptive material, which is not statutory subject matter even if stored in a computer-readable medium. See MPEP § 2106.01.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 1-12, 14, 26, 27, 37, 47-58, 60, and 63 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "using only said key to reveal said embedded digital string in clear form" in lines 12-13 of the claim. The use of the term "only" is generally unclear, as it is not apparent how it further limits the claim; that is, it is not clear what else would be used to reveal the string aside from the key. It appears that the term should be deleted or clarified.

Claim 26 recites the limitation "valued content has been inappropriately distributed". The use of the relative and subjective term "inappropriately" renders the claim indefinite, because the term is not explicitly defined in the claims or specification, nor are examples of what is appropriate or inappropriate distribution provided. See MPEP § 2173.05(b).

Claim 37 recites the limitation "said embedded digital string is extractable in clear form from said second digital file using only said key" in lines 13-14 of the claim. The use of the term "only" is generally unclear, as it is not apparent how it further limits the claim; that is, it is not clear what else would be used to extract the string aside from the key. It appears that the term should be clarified or deleted.

Claim 49 recites the limitation "the encryption keys". There is insufficient antecedent basis for this limitation in the claims.

Claim 50 recites the limitation "using only one of said publicly available encryption keys to reveal said digital string". First, there is insufficient antecedent basis

for the limitation "said publicly available encryption keys" in the claims. Further, the use of the term "only" is unclear, as it is not apparent which particular one of the keys is to be used to reveal the string.

Claim 51 recites the limitation "said computer program". There is insufficient antecedent basis for this limitation in the claims.

Claim 52 recites the limitation "all of the encryption keys"; there does not appear to be sufficient antecedent basis for this limitation in the claims.

Claim 53 recites the limitation "said at least one of the encryption keys". There is insufficient antecedent basis for this limitation in the claims.

Claim 54 recites the limitation "said purchaser is informed by said provider"; however, there is no recitation of what facts or information, for example, of which the purchaser is informed. Further, Claim 54 recites the limitation "the purchase of said valued content". There is insufficient antecedent basis for this limitation in the claims.

Claim 55 recites the limitation "the encryption keys". There is insufficient antecedent basis for this limitation in the claims.

Claim 56 recites the limitation "said digital watermark". There is insufficient antecedent basis for this limitation in the claims.

Claim 57 recites the limitation "a notice of a reward if said valued content is distributed inappropriately". First, the use of the relative and subjective term "inappropriately" renders the claim indefinite, because the term is not explicitly defined in the claims or specification, nor are examples of what is appropriate or inappropriate distribution provided. See MPEP § 2173.05(b). Second, the language of the claim

appears to suggest that the reward is for distributing the content inappropriately, which appears contradictory. This is in contrast to the language in Claim 26 where a reward is for detecting if content is distributed inappropriately.

Claim 58 recites the limitation "to recover said acquired digital string in clear form from only said decryption key and said published first encryption key". The use of the term "only" is generally unclear. In particular, it appears that the claim recites that the string can be recovered using only the two claimed keys, without using the encrypted string; this appears to be contradictory.

Claim 60 recites the limitation "using only one of the publicly available encryption keys to reveal said purchaser digital string in clear form". The use of the term "only" is generally unclear, as it is not clear what else would be used to reveal the string aside from a key.

Claim 63 recites the limitation "at least some of said two or more encoded digital strings". The use of the term "some" renders the claim indefinite, because "some" does not explicitly define a specific quantity or provide any basis for comparison as to how many "some" is intended to represent.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-12, 14, 15, 21-27, 31-34, 37, 42-44, 47-57, and 59-63 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiser et al, US Patent 6385596, in view of Fujiwara, US Patent Application Publication 2001/0054081, and Stefik et al, US Patent 6233684.

In reference to Claim 1, Wiser discloses valued content in a computer readable-medium including a digital file having independent value to a provider (column 6, lines 48-52) and a digital string having a latent value to a purchaser embedded in a passport that is linked to the digital file (column 8, lines 53-56, where the string is personal information). Wiser further discloses that the string is provided in clear form and modified according to a key (column 9, lines 19-20). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at

the time the invention was made modify the content of Wiser to include the string also embedded directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049).

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a system for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used (column 8, lines 51-55). Stefik further discloses that the provider makes the key publicly available and that the file can be processed using the key to reveal the string in clear form (column 16, line 51-column 18, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claims 2, 3, 47, and 48, Wiser, Fujiwara, and Stefik further disclose that the string is encrypted, using a private or public key (Wiser, column 9, lines 19-20; Stefik, column 16, line 51-column 18, line 5).

In reference to Claim 4, Wiser, Fujiwara, and Stefik further disclose the string being embedded in a human perceptible form (Wiser, column 9, lines 16-18; Fujiwara, page 5, paragraph 0049; Stefik, column 8, lines 51-55).

In reference to Claim 5, Wiser, Fujiwara, and Stefik further disclose a digital watermark (Wiser, column 7, lines 5-6 and 17-26; Stefik, column 8, lines 51-55).

In reference to Claims 6-9, Wiser, Fujiwara, and Stefik further disclose that the file can include text, images, video, and audio (Wiser, column 6, lines 59-60, for text and images; Wiser, column 6, lines 48-52; column 7, lines 4-9 for audio; Fujiwara, for example, page 6, paragraph 0057 for text, images, and audio; Stefik, column 5, lines 35-40, for text, images, audio, and video).

In reference to Claim 10, Wiser, Fujiwara, and Stefik further disclose that the latent value of the string resides in information that would place the purchaser at increased financial risk if known by another (Wiser, column 8, lines 53-56).

In reference to Claims 11 and 12, Wiser, Fujiwara, and Stefik further disclose a provider string that can be encrypted (see Wiser, column 4, lines 1-4; column 7, lines 27-46; see also column 10, line 60-column 11, line 7).

In reference to Claim 14, Wiser, Fujiwara, and Stefik further disclose recording the file on a portable medium (see Wiser, column 9, line 53-column 10, line 16).

In reference to Claims 15 and 57, Wiser discloses valued content in a computer readable-medium including a digital file having independent value to a provider (column 6, lines 48-52), a digital string having a latent value to a purchaser embedded in a

passport that is linked to the digital file (column 8, lines 53-56) and is encrypted (column 9, lines 19-20), and an encrypted provider digital string (see column 4, lines 1-4; column 7, lines 27-46). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the content of Wiser to include the string also embedded directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049).

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times. Stefik discloses a system for controlling use of digital works in which multiple watermarks may be embedded within a digital work (column 8, lines 51-55). Stefik also discloses an encrypted provider string (column 3, lines 31-35). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the

invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claim 21, Wiser discloses a method including acquiring a digital string, modifying the digital string (column 9, lines 19-20), embedding the string in a passport that is linked to the digital file (column 8, lines 53-56), and conveying the file to a purchaser (column 9, lines 54-56). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a method for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Wiser to include embedding the string directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049).

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a method for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used, where the multiple watermarking methods form different modified strings (column

8, lines 51-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claims 22-24, Wiser, Fujiwara, and Stefik further disclose encrypting the digital string using public or private keys (Wiser, column 9, lines 19-20; Stefik, column 16, line 51-column 18, line 5).

In reference to Claim 25, Wiser, Fujiwara, and Stefik further disclose generating a digital watermark (Wiser, column 7, lines 5-6 and 17-26; Stefik, column 10, lines 20-22; column 8, lines 51-55).

In reference to Claims 26 and 27, Wiser, Fujiwara, and Stefik further disclose a provider string that can be encrypted (see Wiser, column 4, lines 1-4; column 7, lines 27-46; see also column 10, line 60-column 11, line 7; Stefik column 3, lines 51-55).

In reference to Claims 31-33, Wiser, Fujiwara, and Stefik further discloses that the string can be embedded in images, audio, or video (Wiser, column 6, lines 59-60, for images; Wiser, column 6, lines 48-52; column 7, lines 4-9 for audio; Fujiwara, for example, page 6, paragraph 0057 for images, and audio; Stefik, column 5, lines 35-40, for images, audio, and video).

In reference to Claim 34, Wiser, Fujiwara, and Stefik further disclose that the latent value of the string resides in information that would place the purchaser at increased financial risk if known by another (Wiser, column 8, lines 53-56).

In reference to Claims 49-56, Wiser, Fujiwara, and Stefik further disclose that at least one key and a process to extract the string in clear form is made publicly available by the provider (column 16, line 51-column 18, line 5).

In reference to Claim 37, Wiser discloses a system including a processor (see, for example, Figure 1, Client System 126; see also column 9, lines 40-52), a storage device (for example, see column 10, lines 50-55), an interface, and content including a digital file (column 6, lines 48-52) and a string embedded in a passport that is linked to the digital file (column 8, lines 53-56). Wiser further discloses that the string is provided in clear form and modified according to a key (column 9, lines 19-20). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the system of Wiser to include the string also embedded directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049).

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a system for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used (column 8, lines 51-55). Stefik further discloses that the provider makes the key publicly available and that the file can be processed using the key to reveal the string in clear form (column 16, line 51-column 18, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claims 42 and 43, Wiser, Fujiwara, and Stefik further disclose a point of sale machine and a network connection (Wiser, see column 11, lines 8-13).

In reference to Claim 44, Wiser discloses a system including a processor (column 9, lines 40-52), an interface that requests a digital string (column 8, lines 53-56), and a storage device (for example, column 10, lines 50-55). Wiser further discloses embedding the string in a passport that is linked to a digital file (column 8, lines 53-56). Wiser further discloses that the string is provided in clear form and

modified according to a key (column 9, lines 19-20). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the system of Wiser to embed the string directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049).

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a method for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used, where the multiple watermarking methods form different modified strings (column 8, lines 51-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow

removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claims 59 and 60, Wiser, Fujiwara, and Stefik further disclose two different strings formed using different encryption keys (see Stefik, column 8, lines 51-55 and column 16, line 51-column 18, line 5).

In reference to Claim 61, Wiser, Fujiwara, and Stefik further disclose embedding at least one modified string a plurality of times (Stefik, column 8, lines 51-55).

In reference to Claim 62, Wiser discloses valued content in a computer readable-medium including a digital file having independent value to a provider (column 6, lines 48-52) and a digital string having a latent value to a purchaser embedded in a passport that is linked to the digital file (column 8, lines 53-56, where the string is personal information). Wiser further discloses that the string is provided in clear form and modified according to a key (column 9, lines 19-20). However, although Wiser discloses that the string is embedded in the passport linked to the file (column 6, lines 44-46), Wiser does not explicitly disclose also embedding the personal information in the file itself.

Fujiwara discloses a system for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the content of Wiser to include the string also

embedded directly in the digital file, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049).

Although Wiser and Fujiwara disclose watermarks (Wiser, column 7, lines 5-6 and 17-26) and a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a system for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used (column 8, lines 51-55). Stefik further discloses that the provider makes the key publicly available and that the file can be processed using the key to reveal the string in clear form (column 16, line 51-column 18, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Wiser and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness; that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claim 63, Wiser, Fujiwara, and Stefik further disclose two different strings formed using different encryption keys (see Stefik, column 8, lines 51-55 and column 16, line 51-column 18, line 5)

10. Claims 36 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dwork et al, US Patent 6038316, in view of Fujiwara and Stefik.

In reference to Claim 36, Dwork discloses acquiring a digital string (column 7, lines 40-47), encrypting a digital string and embedding the string in a decryption key (column 7, lines 14-19), encrypting a digital file (column 7, lines 34-37), and conveying the encrypted file to a purchaser (column 7, lines 38-40). However, Dwork does not explicitly disclose also embedding the digital string in the digital file that is encrypted.

Fujiwara discloses a method for content delivery in which personal data is embedded in a delivered digital file (page 4, paragraph 0047; page 5, paragraphs 0049 and 0054). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made modify the method of Dwork to include embedding the string directly in the digital file before encryption, in order to effectively prevent illegal copying (see Fujiwara, page 5, paragraph 0049).

Although Dwork and Fujiwara disclose a string embedded in a digital file (Fujiwara, page 4, paragraph 0047; page 5, paragraphs 0049 and 0054), neither Wiser nor Fujiwara explicitly discloses embedding the string multiple times nor in a hidden manner. Stefik discloses a method for controlling use of digital works in which multiple watermarks may be embedded within a digital work, and both visible and invisible (i.e. hidden) watermarks may be used (column 8, lines 51-55). Stefik further discloses that the provider conveys a key to the public and that the file can be processed using the key to reveal the string in clear form (column 16, line 51-column 18, line 5). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the content of Dwork and Fujiwara to include the string embedded two or more times, at least once in a hidden manner, in order to increase robustness;

that is, even if the visible string(s) is/are somehow removed, the invisible one(s) would remain and still allow control of the digital rights (see Stefik, column 8, lines 55-56).

In reference to Claim 58, Dwork, Fujiwara, and Stefik further disclose that a process to recover the string in clear form is conveyed to the public (column 16, line 51-column 18, line 5).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

Matthew B. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137